

WHAT IS CLAIMED IS:

1. A digital watermark embedding apparatus comprising:

a first embedding block which embeds a first digital watermark in a host data; and

a second embedding block which embeds information on watermarking location of the first digital watermark, as a second watermark, into the host data in which the first digital watermark has been embedded.

2. The apparatus of Claim 1, wherein the first embedding block comprising:

a location information generating unit which generates a plurality of candidate locations of the host data in which the first digital watermark is to be embedded;

a first embedding unit which embeds the first digital watermark in the respective candidate locations of the host data and generates a plurality of candidates for a first watermarked host data;

a first evaluating unit which evaluates robustness of the first digital watermark hidden in the respective candidates for the first watermarked host data; and

a first selecting unit which selects one of the plurality of the candidates for the first watermarked host data according to the evaluated robustness and outputs the selected one as the host data in which the first digital

watermark is embedded.

3. The apparatus of Claim 1, wherein the second embedding block comprising:

a scrambling unit which scrambles the information on the watermarking location and generates a plurality of candidate watermarks;

a second embedding unit which embeds the respective candidate watermarks in the host data in which the first digital watermark has been embedded and generates a plurality of candidates for a second watermarked host data;

a second evaluating unit which evaluates robustness of the respective candidate watermarks hidden in the respective candidates for the second watermarked host data; and

a second selecting unit which selects one of the plurality of the candidates for the second watermarked host data according to the evaluated robustness.

4. The apparatus of Claim 3, wherein the second embedding unit restricts the candidates for the second watermarked host data to be within an acceptable degradation range for the host data after the first digital watermark is embedded and to be within an acceptable degradation range for the original host data before the first digital watermark is embedded.

5. The apparatus of Claim 4, wherein the second embedding

unit relaxes a restriction so that a part of watermarked samples of the candidates for the second watermarked host data is allowed to be out of the acceptable degradation range for the original host data before the first digital watermark is embedded.

6. A digital watermark extracting apparatus comprising:

- a first extracting block which extracts a first digital watermark from a twice-watermarked host data and translates the first digital watermark into information on watermarking location of a second watermark;

- a removing unit which removes the first digital watermark from the host data; and

- a second extracting block which extracts the second digital watermark from the host data from which the first digital watermark has been removed by the removing unit according to the information on the watermarking location.

7. The apparatus of Claim 6, wherein the first extracting block comprising:

- an extracting unit which extracts a scrambled watermark from the twice-watermarked host data; and

- a descrambling unit which descrambles the scrambled watermark and obtains the information on the watermarking location of the second watermark.

8. A digital watermark extracting apparatus comprising:

a first extracting block which extracts a first digital watermark from a twice-watermarked host data;

a first removing unit which removes the first digital watermark from the host data;

a second extracting block which lies immediately posterior to the first extracting block and extracts a second digital watermark from the host data from which the first digital watermark has been removed by the first removing unit; and

a second removing unit which removes the second digital watermark from the host data,

wherein the host data from which the second digital watermark has been removed by the second remover is feedback to the first extracting block, and the first extracting block extracts the first digital watermark from the host data from which the second digital watermark has been removed, and thereby the first digital watermark and the second digital watermark are iteratively decoded in sequence.

9. The apparatus of Claim 8, wherein the first extracting block includes a soft-output decoding unit which performs soft decision decoding on the first digital watermark and outputs a soft decision value of the first digital watermark, and the first remover removes the first digital watermark formed by the soft decision value from the host data.

10. The apparatus of Claim 9, wherein the second extracting block includes a soft-output decoding unit which performs soft decision decoding on the second digital watermark and outputs a soft decision value of the second digital watermark, and the second remover removes the second digital watermark formed by the soft decision value from the host data.

11. A digital watermark extracting apparatus comprising:

- a first extracting block which extracts a first digital watermark from a twice-watermarked host data;

- a first removing unit which removes the first digital watermark from the host data;

- a second extracting block extracts a second digital watermark from the host data; and

- a second removing unit which removes the second digital watermark from the host data,

wherein the host data from which the second digital watermark has been removed by the second remover is feedback to the first extracting block, and the first extracting block extracts the first digital watermark from the host data from which the second digital watermark has been removed, and the host data from which the first digital watermark has been removed by the first remover is feedback to the second extracting block, and the second extracting block extracts the second digital watermark from the host data from which

the first digital watermark has been removed, and thereby the first digital watermark and the second digital watermark are iteratively decoded in parallel.

12. The apparatus of Claim 11, wherein the first extracting block includes a soft-output decoding unit which performs soft decision decoding on the first digital watermark and outputs a soft decision value of the first digital watermark, and the first remover removes the first digital watermark formed by the soft decision value from the host data.

13. The apparatus of Claim 12, wherein the second extracting block includes a soft-output decoding unit which performs soft decision decoding on the second digital watermark and outputs a soft decision value of the second digital watermark, and the second remover removes the second digital watermark formed by the soft decision value from the host data.

14. A data structure of a twice-watermarked host data readable and usable by a computer comprising two embedded digital watermarks, wherein information on watermarking location of a first digital watermark is embedded as a second digital watermark by a reversible watermarking method.

15. A digital watermark extracting method comprising extracting a first digital watermark embedded by a reversible

watermarking method from a twice-watermarked host data and removing the extracted first digital watermark from the host data and thereafter extracting a second digital watermark from the host data from which the first watermark has been removed.

16. The method of Claim 15, wherein the first digital watermark is meta-information for identifying a watermarking method of the second digital watermark and the second digital watermark is extracted from the host data by a method identified by the meta-information.

17. A method for doubly watermarking a host data, comprising embedding information on watermarking location of a first digital watermark as a second watermark into the host data by a reversible watermarking method.

18. A method for embedding two digital watermarks containing information with different degrees of importance into a host data, comprising embedding one digital watermark containing more important information with a higher degree of robustness into the host data.

19. The method of Claim 18, wherein the digital watermark containing more important information is embedded into the host data by a reversible watermarking method.

20. A computer program executable by a computer, the program comprising:

- extracting a first digital watermark from a twice-watermarked host data and translating the first digital watermark into information on watermarking location of a second watermark;

- removing the first digital watermark from the host data; and

- extracting the second digital watermark from the host data from which the first digital watermark has been removed according to the information on the watermarking location.

21. A method for extracting two digital watermarks in sequence from a twice-watermarked host data by iterative decoding, comprising:

- a first watermark extracting process which estimates a first digital watermark from the twice-watermarked host data and removes the estimated first digital watermark from the twice-watermarked host data;

- a second watermark extracting process which estimates a second digital watermark from the host data from which the estimated first digital watermark has been removed and removes the estimated second digital watermark from the twice-watermarked host data; and

- a feedback process which feedbacks the host data from

which the estimated second watermark has been removed to the first watermark extracting process,

wherein the first watermark extracting process estimates the first digital watermark from the twice-watermarked host data at a first iteration of the iterative decoding, and estimates the first digital watermark from the host data from which the estimated second digital watermark has been removed at a second iteration and afterwards.

22. The method of Claim 21, wherein the first watermark extracting process performs soft decision decoding on the first digital watermark and removes the first digital watermark formed by a soft decision value from the host data.

23. The method of Claim 22, wherein the second watermark extracting process performs soft decision decoding on the second digital watermark and removes the second digital watermark formed by a soft decision value from the host data.

24. A method for extracting two digital watermarks in parallel from a twice-watermarked host data by iterative decoding, comprising:

a first watermark extracting process which estimates a first digital watermark from the twice-watermarked host data and removes the estimated first digital watermark from the twice-watermarked host data;

a second watermark extracting process which estimates a second digital watermark from the twice-watermarked host data and removes the estimated second digital watermark from the twice-watermarked host data;

a feedback process which feedbacks the host data from which the estimated second watermark has been removed to the first watermark extracting process; and

a feedback process which feedbacks the host data from which the estimated first watermark has been removed to the second watermark extracting process,

wherein the first watermark extracting process estimates the first digital watermark from the twice-watermarked host data at a first iteration of the iterative decoding, and estimates the first digital watermark from the host data from which the estimated second digital watermark has been removed at a second iteration and afterwards, and

wherein the second watermark extracting process estimates the second digital watermark from the twice-watermarked host data at a first iteration of the iterative decoding, and estimates the second digital watermark from the host data from which the estimated first digital watermark has been removed at a second iteration and afterwards.

25. The method of Claim 24, wherein the first watermark extracting process performs soft decision decoding on the first digital watermark and removes the first digital

watermark formed by a soft decision value from the host data.

26. The method of Claim 25, wherein the second watermark extracting process performs soft decision decoding on the second digital watermark and removes the second digital watermark formed by a soft decision value from the host data.